UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/524,583 | 02/15/2005 | Mats Naslund | P17238-US1 | 6534 |

27045 7590 08/05/2008

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

| EXAMINER | |
|---|---|
| YOUSEFI, SHAHROUZ | |
| **ART UNIT** | **PAPER NUMBER** |
| 2132 | |
| **MAIL DATE** | **DELIVERY MODE** |
| 08/05/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/524,583 | NASLUND ET AL. | |
| | Examiner | Art Unit | |
| | SHAHROUZ YOUSEFI | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 February 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/15/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 101*

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 28-46 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Data structures not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable, per se, of causing functional change in the computer. See MPEP 2106.01 and e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760.

### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-13, 15-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Lindholm et al. (US 2004/0117500) hereinafter Lindholm.

5. With respect to claims 1 and 15, Lindholm discloses a tamper-resistant identity module (**tamper resistant integrated circuit, par. [0091]**) adapted for physical

engagement with a client system (**included in the client 1, par. [0091]**) having means for receiving digital content (**streaming media, par. [0053]**) over a network (**elementary network, par. [0053**) and a digital-content usage device (**Means for rendering streaming data on a display and/or by loudspeaker, par. [0062])**, wherein said tamper-resistant identity module comprises a digital rights management DRM agent (**DRM module 41, par. [0093]**) for enabling usage of said digital content.

6. With respect to claims 2 and 16, Lindholm discloses said DRM agent is implemented as an application in an application environment of said tamper-resistant identity module (The DRM module 41 in the Client, par. [0103] and par. [0091]).

7. With respect to claims 3 and 17, Lindholm discloses said DRM agent application is loaded into said identity module application environment from an external trusted party associated with said identity module (the client ordering the media from the order server, the order server handling the media order and the streaming server delivering the streaming media to the client, par. [0041]).

8. With respect to claims 4 and 18, Lindholm discloses said identity module comprises means for authenticating said DRM agent (Authentication of the client, par. [0038] and a field 24 for authentication information, par. [0088]).

9. With respect to claims 5 and 19, Lindholm discloses means for performing at least part of an authentication and key agreement (AKA) procedure, and said DRM agent includes means for performing DRM processing based on information from said AKA procedure (To provide trust management in the case where there is no pre-existing relation, and/or authentication between the communicating parties the following optional

"certificate" structure can be used, as illustrated by the block diagram of FIG. 3, par. [0098]).

10. With respect to claims 6 and 20, Lindholm discloses said DRM agent includes means for extracting a content-protection key to be used for decrypting encrypted digital content provided from a content provider, based on information from said AKA procedure (From the ticket, the Client 1 extracts the data, most importantly the session key, and forwards it in encrypted shape to the Streaming Server 5 along with the authorization of the Order Server, i.e. the signature/authentication tag of the Order Server, par. [0103]).

11. With respect to claims 7 and 21, Lindholm discloses said DRM agent comprises means for enabling charging for digital content usage (A charging service, par. [0034] and par. [0063]).

12. With respect to claim 8, Lindholm discloses said DRM agent comprises means for managing information related to usage of said digital content, said usage information serving as a basis for charging for digital-content usage (This request may also contain additional information for charging purposes, such as means of payment, credit card number or other monetary information and desired usage of the streaming data, such as duration, format of media, etc., par. [0065]).

13. With respect to claim 9, Lindholm discloses means for integrity protecting said usage information based on an identity-module specific key; and means for sending said integrity protected usage information to an external party managing charging of digital-content usage (The Order Server OS 3 handles the requests from the Client and

manages primarily the charging related to the requested media, see also the block diagram of FIG. 7. The Streaming Server 5, see also the block diagram of FIG. 8, houses and manages the streaming data according to conditions set by the Order Server and by the Client, par. [0063] and par. [0068]).

14. With respect to claim 10, Lindholm discloses said DRM agent implemented in said identity module further comprises means for enabling registration of at least one digital-content usage device (the Order Server 3 is managed by an operator, the Order Server may check whether the equipment is registered in a database, par. [0100]).

15. With respect to claims 11 and 22, Lindholm discloses means for communication between said DRM agent and further DRM functionality implemented in said digital-content usage device based on usage-device specific key information (Before the Client 1 actually orders some media object some actions may be taken in communicating between the Client and the Order Server 3, such as finding information on media type, quality, pricing, previewing, etc, par. [0070]).

16. With respect to claim 12 and 23, Lindholm discloses said communication means is operable for ensuring that only a usage device with valid DRM functionality is enabled to use said digital content (The Client 1 is involved in communication with the Order Server 3 resulting in a formal order… exchange of security information, such as authentication of the Client, to be used in the order process and/or in the charging process and/or in the ticket creation process to be described below, par. [0071]).

17. With respect to claim 13, Lindholm discloses means for receiving, from an external trusted party, a DRM application adapted for use with a digital-content usage

device, and means for transferring said DRM application into a tamper-resistant application environment in said digital-content usage device based on usage-device specific key information (The method and network offer a simple way of distributing material protected by copyright that is adapted to streaming purposes, real-time, possibly interactive data transfer being a special case. By using a robust protocol in the method and network, they are much more suited for wireless clients and heterogeneous environments than existing solutions. The advantage of using a standardized protocol, like SRTP, WTLS, etc., is that it can be implemented in many devices not only for the purpose of Digital Rights Management and therefore can be reused to significantly save storage capacity, par. [0042]).

18. With respect to claim 24, Lindholm discloses means for transmitting, to a trusted certification party, identification information associated with said digital-content usage device, and in response thereto receiving a protected representation of said usage-device specific key (In fact, manufacturers may obtain security certification of their products, par. [0045]), and said DRM agent comprises means for extracting said usage-device specific key representation for storage in said tamper-resistant identity module (From the ticket, the Client 1 extracts the data, most importantly the session key, and forwards it in encrypted shape to the Streaming Server 5 along with the authorization of the Order Server, i.e. the signature/authentication tag of the Order Server, par. [0103]).

19. With respect to claim 25, Lindholm discloses said digital-content usage device includes a tamper-resistant application environment (The DRM module 41 in the Client, par. [0103] and par. [0091]), and a DRM application adapted for use as a DRM agent in

said usage device is loaded into said application environment at least partly based on usage-device specific key information (the client ordering the media from the order server, the order server handling the media order and the streaming server delivering the streaming media to the client, par. [0041]).

20. With respect to claim 26, Lindholm discloses means for generating new device key information associated with a downloaded DRM application at least partly based on said usage-device specific key information (If the Client 1 has a known public key, the Order Server 3 may leave the generation of the session key to the Streaming Server 5, and the tickets may not carry this information, par. [0081]); and means for replacing usage-device specific key information stored in said usage device with said new device key information (From the ticket, the Client 1 extracts the data, most importantly the session key, and forwards it in encrypted shape to the Streaming Server 5 along with the authorization of the Order Server, i.e. the signature/authentication tag of the Order Server, par. [0103]).

21. With respect to claim 27, Lindholm discloses said DRM agent implemented in said identity module comprises means for replacing usage-device specific key information stored in said identity module with key information corresponding to said new device key information (a key distribution mechanism, par. [0033]).

22. Claims 1, 14, and 28-47 are rejected under 35 U.S.C. 102(e) as being anticipated by Kontio et al. (US 2004/0249768) hereinafter Kontio.

23. With respect to claim 28, Kontio discloses a first DRM agent implemented in a tamper-resistant identity module (“**first DRM agent”, par. [0052] and “tamper**

**resistance techniques, persistently protecting the content using encryption techniques", par. [0149]**) for engagement with a client device (**a DRM agent...for obtaining information about the content from the voucher server, par. [0050]**), said first DRM agent comprising means for performing first DRM processing associated with digital content (**The DRM agent responds by sending an offer of consideration to the wireless device, including consideration information obtained from the voucher server, par. [0050]**); a second DRM agent implemented in a digital-content usage device adapted for using said digital content, said second DRM agent comprising means for performing second DRM processing associated with said digital content (**In an alternate embodiment of the invention, the terminal device sends and give voucher to a second DRM agent in the network, different from the first DRM agent par. [0052]**); and means for communication between said first DRM agent and said second DRM agent based on usage-device specific key information (**distributing terminal 100 and receiving terminal 140, fig. 1, and FIG. 2 is a network diagram that expands the system shown in FIG. 1 by illustrating the communication between retail content service 110 and receiving terminal 140, par. [0088]**).

24. With respect to claim 29, Kontio discloses said communication means is operable for ensuring that only a usage device with valid DRM functionality is enabled to use said digital content (FIG. 2 is a network diagram that expands the system shown in FIG. 1 by illustrating the communication between retail content service 110 and receiving terminal 140, par. [0088]).

25. With respect to claim 30, Kontio discloses said tamper-resistant identity module comprises means for performing at least part of an authentication and key agreement (AKA) procedure (methods to generate and evaluate message authentication codes to insure the integrity of data, par. [0246]), and said means for performing first DRM processing in said first DRM agent operates based on information from said AKA procedure (the DRM agent responds by sending an offer of consideration to the wireless device, including consideration information obtained from the voucher server, par. [0050]).

26. With respect to claim 31, Kontio discloses said means for performing first DRM processing in said first DRM agent includes means for extracting a content-protection key to be used for decrypting protected digital content from a content provider, based on information from said AKA procedure (the voucher including a pointer to the content, use information specifying the type of use intended for the content, restriction information limiting usage of the content, and protection information specifying an ID for the content and an encryption key for the content, par. [0049]).

27. With respect to claim 32, Kontio discloses said communication means is operable for ensuring that said content-protection key is accessible only by a second DRM agent that properly enforces usage rules associated with said digital content (when the user carries receiving terminal 140 into the communications range of retail content service 110, the user can browse the content of retail content service 110, par. [0089]).

28. With respect to claim 33, Kontio discloses said means for performing second DRM processing in said second DRM agent comprises means for decrypting encrypted digital content by means of said content-protection key (In practice this means that the content is encrypted and the decryption key is only available for those terminals that have paid to consume the content, par. [0376]).

29. With respect to claim 34, Kontio discloses said means for performing first DRM processing in said first DRM agent comprises means for enabling charging for said digital content (Payment or charging solutions, with the exception of some electronic payment solutions, normally require network interaction with a charging server of some sort, par. [0212]).

30. With respect to claim 35, Kontio discloses said first DRM agent comprises: means for authenticating said usage device based on said usage-device specific key information to verify that said usage device has valid DRM functionality (methods to generate and evaluate message authentication codes to insure the integrity of data, par. [0246]); means for sending DRM data enabling usage of said digital content to said second DRM agent in response to successful authentication of a usage device with valid DRM functionality (In an alternate embodiment of the invention, the terminal device sends and give voucher to a second DRM agent in the network, different from the first DRM agent par. [0052]).

31. With respect to claim 36, Kontio discloses said first DRM agent comprises: means for encrypting DRM data enabling usage of said digital content, based on said usage-device specific key information (The voucher server encrypts the content with a

content key, par. [0053]); and means, forming part of said communication means, for sending said encrypted DRM data to said second DRM agent; and said second DRM agent comprises means for decrypting said encrypted DRM data to enable usage of said digital content, based on said usage-device specific key information (the terminal device sends and give voucher to a second DRM agent in the network, different from the first DRM agent par. [0052]).

32. With respect to claim 37, Kontio discloses said tamper-resistant identity module and said usage device are tamper-resistantly configured with usage-device specific key information (Several techniques are disclosed to protect the content and the content key. In one embodiment, the wireless device is enabled to recover the content key to decrypt the encrypted content, par. [0053]).

33. With respect to claim 38, Kontio discloses said second DRM agent comprises means for compiling information related to usage of said digital content, and means for transferring said usage information to said first DRM agent based on said usage-device specific key information; and said first DRM agent comprises means for sending said usage information to an external party managing charging of digital-content usage, said usage information serving as a basis for charging for digital-content usage (the terminal device sends and give voucher to a second DRM agent in the network, different from the first DRM agent par. [0052]).

34. With respect to claim 39, Kontio discloses said second DRM agent comprises means for sending a first control signal related to the digital-content usage process to said first DRM agent, and said first DRM agent comprises means for processing signal

data associated with said first control signal to generate a second control signal, and means for sending said second control signal to said second DRM agent for controlling said digital-content usage process, par. [0052].

35. With respect to claim 40, Kontio discloses said first DRM agent is implemented as an application in an application environment of said tamper-resistant identity module (Solutions include hardware and tamper resistance techniques, persistently protecting the content using encryption techniques such as RSA or Diffie-Hellman encryption, and a combination of tamper resistance and encryption, par. [0149]).

36. With respect to claim 41, Kontio discloses said first DRM agent application is loaded into said identity module application environment from an external trusted party associated with said identity module (The settlement process is external to the DRM system and can be implemented by interfacing with existing invoicing systems, par. [0347]).

37. With respect to claim 42, Kontio discloses said identity module comprises means for authenticating said DRM agent (methods to generate and evaluate message authentication codes to insure the integrity of data, par. [0246]).

38. With respect to claim 43, Kontio discloses second DRM agent is implemented as an application in a tamper-resistant application environment in said usage device (second DRM agent in the network, par. [0052]).

39. With respect to claim 44, Kontio discloses said second DRM agent application is loaded into said usage-device application environment at least partly based on said usage-device specific key information, par. [0052].

40. With respect to claim 45, Kontio discloses means for generating new device key information associated with said downloaded DRM application at least partly based on said usage-device specific key information ("content encryption key generation, optionally content ID generation", par. [0302] and "The function of this interface is to perform terminal initialization (e.g., key generation), terminal renovation (e.g., key refresh, DRM client binary update), and terminal revocation", par. [369]); and means for replacing usage-device specific key information stored in said usage device with said new device key information (Mutate the metadata to reflect changes to rights and rules associated with content and user, par. [0268]).

41. With respect to claim 46, Kontio discloses said DRM agent implemented in said identity module comprises means for replacing usage-device specific key information stored in said identity module with key information corresponding to said new device key information (A rights gateway such as rights gateway 1120 can perform the following operations on the metadata: par. [0267] 1. Mutate the metadata to reflect changes to rights and rules associated with content and user, par. [0268] 2. Obtain payment authorization to change the rights portion of metadata, par. [0269]).

42. With respect to claim 47, Kontio discloses a method for digital rights management (DRM) ("**DRM agent", par. [0052]**) comprising the steps of: tamper-resistantly configuring a usage device (**"tamper resistance techniques, persistently protecting the content using encryption techniques", par. [0149]**), adapted for using digital content, with a usage-device specific key **("content encryption key generation, optionally content ID generation", par. [0302]**); providing a

cryptographic representation of said usage-device specific key to a client device associated with said usage device (**The function of this interface is to get terminal cryptographic information of a specific terminal (e.g., symmetric key, public key or certificate) and to check revocation status of a specific terminal, par. [0368]**); processing, at a trusted certification party (**implementing a DRM architecture in an open or trusted computing environment, par. [0010]**), said cryptographic representation received in a request from said client device to retrieve key information representative of said usage-device specific key (In practice this means that the content is encrypted and the decryption key is only available for those terminals that have paid to consume the content, par. [0376]); securely transferring said key information from said trusted certification party to a tamper-resistant identity module in said client device, based on an identity-module specific key (a certificate including a signing key for the buyer device and a charge authorization ticket, par. [0047]); establishing communication between a first DRM agent in said tamper-resistant identity module and a second DRM agent in said usage device based on the key information transferred to the identity module and the usage-device specific key in said usage device (distributing terminal 100 and receiving terminal 140, fig. 1, and FIG. 2 is a network diagram that expands the system shown in FIG. 1 by illustrating the communication between retail content service 110 and receiving terminal 140, par. [0088]).

43. With respect to claim 1, Kontio discloses a tamper-resistant identity module (**tamper resistance techniques, persistently protecting the content using encryption techniques", par. [0149]**) adapted for physical engagement with a client

system (**a DRM agent…for obtaining information about the content from the voucher server, par. [0050]**) having means for receiving digital content (**a receiving terminal in the non-personalized Mobile Rights Voucher copy intent process for sending a preview copy of protected digital content, par. [0068]**) over a network (**digital communication network, par. [0013]**) and a digital-content usage device (**tracking asset usage, par. [0009]**), wherein said tamper-resistant identity module comprises a digital rights management DRM agent (**DRM agent, par. [0052]**) for enabling usage of said digital content.

44. With respect to claim 14, Kontio discloses means for checking that the forward-lock function of the Wireless Application Protocol (WAP) is not violated (Today copy protection is done in the mobile domain with so called forward-lock method in which the terminal disables the ability to forward the piece of content (e.g. ringing-tone) to another terminal, par. [0278]).

## Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHAHROUZ YOUSEFI whose telephone number is (571) 270-3558. The examiner can normally be reached on Monday-Thursday 9:00-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. Y./
Examiner, Art Unit 2132

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132